Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0584-2009

for

NXP P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software

from

NXP Semiconductors Germany GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0584-2009

NXP P5CC036V1D Secure Smart Card Controller
with Cryptographic Library as IC Dedicated Support Software

from	NXP Semiconductors Germany GmbH
PP Conformance:	Smartcard IC Platform Protection Profile, Version 1.0, BSI-PP-0002-2001
Functionality:	BSI-PP-0002-2001 conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Common Criteria
Recognition
Arrangement
for components up to
EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 3 June 2009

For the Federal Office for Information Security

IT
Security
Certified

SOGIS - MRA

Bernd Kowalski L.S.
Head of Department

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

This evaluation contains the components ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product NXP P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0296-2005. Specific results from the evaluation process BSI-DSZ-CC-0296-2005 were re-used.

The evaluation of the product NXP P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software was conducted by T-Systems GEI GmbH. The evaluation was completed on 06 April 2009. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

[6] Information Technology Security Evaluation Facility

For this certification procedure the applicant is: NXP Semiconductors Germany GmbH

The product was developed by: NXP Semiconductors Germany GmbH

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product NXP P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] NXP Semiconductors Germany GmbH
P.O. Box 54 02 40
22502 Hamburg
Germany

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) and subject of the Security Target (ST) [6] resp. [9] is the NXP P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software .

The evaluation of the TOE was conducted as a composition evaluation making use of the platform evaluation results of the CC evaluation of the underlying semiconductor.

Therefore, the Target of Evaluation (TOE) consists of a hardware part and a software part. The hardware part consists of the NXP P5CC036V1D with IC Dedicated Software stored in the Test-ROM that is not accessible in the System Mode or the User Mode after Phase 3. There is dedicated documentation regarding the hardware. The additional IC Dedicated Support Software "Secured Crypto Library on the P5CC036V1D" consists of a software library and associated documentation. The Secured Crypto Library provides cryptographic functions that can be operated on the hardware platform as described in the Security Target lite [6] resp. [9].

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Smartcard IC Platform Protection Profile, Version 1.0, BSI-PP-0002-2001 [10].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Assurance Requirements of the Evaluation Assurance Level EAL 4 augmented by ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 5.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6] and [9], chapter 5.2.

The TOE Security Functional Requirements are implemented by the following TOE Security Functions:

TOE Security Function	Addressed issue
F.RNG_Access	Software generation of random numbers and test functionality for hardware RNG
F.DES	DES and TDES encryption and decryption in ECB, "outer" CBC and CBC-MAC mode
F.RSA	RSA and RSA-CRT algorithms
F.RSA_KeyGen	Key generation for the RSA
F.SHA-1	Computation of the SHA-1 algorithm
F.LOG	Extends the F.LOG of hardware part of the TOE and provides in addition protection against side channel attacks and forced leakage attacks for the additional functionality F.DES, F.RSA, F_.RSA, F.Rsa:Keygen
F.COPY	Provides means to copy of data resistant to side channel attacks
F.Object_Reuse	Clears memory areas used by the crypto library after usage

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] and [9], chapter 6.1.

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6] and [9], chapter 6 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapter 3.

- Major configuration NXP P5CC036V1D has the following properties that are relevant with regard to the configuration: The size of the EEPROM is 36 kBytes, the size of the ROM usable for the Smart Card Embedded Software is 128 kBytes.
- Secured Crypto Library on the P5CC036V1D.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

NXP P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Date	Form of Delivery
1	HW	NXP P5CC036V1D Secure Smart Card Controller	V1D	T503D.gds2_ 20040915	Wafer, (dice include reference T503D)
2	SW	Test ROM Software (the IC dedicated Test Software)	1.4	2004-08-16	test ROM on the chip (tmfos.lst, V1.4)
3	SW	Boot ROM Software (part of the IC dedicated Support Software)	1.7 boot.asm	2004-03-09	test ROM on the chip (tmfos.lst, V1.4)
4	DOC	Data Sheet, P5CC036 [12]	3.3	2005-06-27	electronic document
5	DOC	Instruction Set [13]	1.1	2006-07-04	electronic document
6	DOC	Guidance, Delivery and Operation Manual for the P5CC009V1D, P5CC036V1D [14]	1.2	2009-01-08	electronic document
7	SW	Secured Crypto Library on the P5CC036V1D Pseudo Random Number Generator	2.0	n/a	Binary library file(s) plus the required header file(s), on CD or electrically

No	Type	Identifier	Release	Date	Form of Delivery
8	SW	Secured Crypto Library on the P5CC036V1D Secured DES Library	1.0	n/a	Binary library file(s) plus the required header file(s), on CD or electrically
9	SW	Secured Crypto Library on the P5CC036V1D Secured RSA Library	2.0	n/a	Binary library file(s) plus the required header file(s), on CD or electrically
10	SW	Secured Crypto Library on the P5CC036V1D Secured RSA Key Generation Library	2.0	n/a	Binary library file(s) plus the required header file(s), on CD or electrically
11	SW	Secured Crypto Library on the P5CC036V1D SHA-1 Library	2.0	n/a	Binary library file(s) plus the required header file(s), on CD or electrically
12	DOC	see [12]-[14] in the bibliography	see bibliography		lectronic document
13	DOC	see [15]-[20] in the bibliography	see bibliography		printed on paper or electronically with the crypto library

Table 2: Deliverables of the TOE

The hardware part of the TOE is not described in detail in this document. The hardware part of the TOE is identified by P5CC036V1D and its specific GDS-file. A so-called nameplate (on-chip identifier) is coded in a metal mask onto the chip during production and can be checked by the customer, too. The nameplate T503D is specific for the SSMC (Singapore) production site as outlined in the guidance documentation [14]. Details are included in the Hardware Security Target [29] resp. [30] and therefore this latter document will be cited where ever appropriate.

The additional IC Dedicated Support Software "Secured Crypto Library on the P5CC036V1D " is part of the TOE. It provides cryptographic support for the NXP P5CC036V1D smart card processor. The IC Dedicated Support Software as part of the TOE provides an interface between the smart card hardware (P5CC036V1D) and a smart card operating system or smart card application for the usage of the cryptographic functions provided by the TOE. It uses the specific functionality of the hardware to provide these cryptographic services.

The crypto library provides DES, Triple-DES (3DES), RSA, RSA-CRT, RSA key generation and SHA-1 algorithms. Both DES and Triple-DES can be used in one of the following modes of operation: ECB, CBC or CBC-MAC. In addition, the crypto library implements a software (pseudo) random number generator which is initialized (seeded) by the hardware random number generator of the SmartMX.

3 Security Policy

The security policy of the TOE is to provide basic security functions to be used by the smart card operating system and the smart card application thus providing an overall smart card system security. Therefore, the TOE will implement a symmetric cryptographic block cipher algorithm (Triple-DES) to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a random number generation of appropriate quality.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during cryptographic functions performed by the TOE), protection against physical probing, malfunctions, physical manipulations, against access for code and data memory and against abuse of functionality.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Details can be found in the Security Target [6] and [9] chapter 4.2.

The smart card applications need the security functions of the smart card operating system based on the security features of the TOE. With respect to security a composition evaluation of the present TOE and the future operating system and smart card application is important. Within the present composition, the security functionality is only partly provided by the TOE and causes dependencies between the TOE security functions and the functions provided by the future operating system or the smart card application on top. These dependencies are expressed by environmental and secure usage assumptions as outlined in the user documentation.

5 Architectural Information

The TOE is a crypto library implemented on the Secure Smart Card Controller NXP P5CC036V1D. The TOE is provided as binary library files plus the required header files to the end-user (embedded software developer) in form of a CD or in another electronically way.

The additional IC Dedicated Support Software "Secured Crypto Library on the NXP P5CC036V1D" is part of the present composite TOE. It provides cryptographic support for the NXP P5CC036V1D smart card processor. The IC Dedicated Support Software as part of the TOE provides an interface between the smart card hardware and a future smart card operating system or smart card application that use the cryptographic functions provided by the TOE. The IC Dedicated Support Software uses the specific functionality of the hardware to provide these cryptographic services.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

Tests were performed in three cathegories:

- Developer's Test according to ATE_FUN: The overall goal of the tests is to show that the TOE implements the TSF as described by the security target and the functional specification. Since SF.Hardware is covered by the HW certification, the testing approach has been to verify that the recommendations from HW to the SW granted by the HW guidance are fulfilled by the embedded software instead of doing functional testing of the HW security functions again.

- Evaluator's Test according to ATE_IND: The testing by itself concentrates on the interface of the security functions.

- To verify and reject possible vulnerabilities, the evaluators performed penetration tests. Therefore, they took all security functions into consideration. Intensive penetration testing was performed to consider the physical tampering of the TOE using highly sophisticated equipment and expertise know how. In addition non-invasive attacks like side channel analysis and fault analysis were performed during the vulnerability tests. During the evaluator's penetration testing the TOE operated as specified. The TOE withstood the penetration efforts of attackers with high attack potential in the intended environment for the TOE.

8 Evaluated Configuration

The TOE is a composite TOE, consisting of the hardware “Philips SmartMX P5CC036V1D Secure Smart Card Controller”, which is used as the evaluated platform and the “Secured Crypto Library on the P5CC036V1D”, which is built upon this platform.

The considered configuration of the Secured Crypto Library on the P5CC036V1D assumes that the crypto library is executed in System Mode.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product [4] (AIS 34).

For smart card IC specific methodology the CC supporting documents

(i) *Functionclasses and methology for deterministic RNGs*

(ii) *The Application of CC to Integrated Circuits*

(iii) *Application of Attack Potential to Smartcards*

(iv) *ETR-lite – for Composition and*
ETR-lite – for Composition: Annex A Composite smartcard evaluation: Recommended best practice

(v) *Functionclasses and methology for nondeterministic RNGs*

(see [4], AIS 20, AIS 25, AIS 26, AIS 31 and AIS 36]) were used.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL 4 package as defined in the CC (see also part C of this report)
- The components ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0296-2005, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on optimized security features.

The evaluation has confirmed:

- PP Conformance: Smartcard IC Platform Protection Profile, Version 1.0, BSI-PP-0002-2001 [10]
- for the Functionality: BSI-PP-0002-2001 conformant
  plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by
  ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function : high
  - The TSF F.LOG – Logical Protection defined in the Hardware Security Target [29] resp. [30] is extended in this Security Target to include software countermeasures against side channel attacks. Such attacks can be performed by externally measuring the power consumption of the SmartMX processor (Simple Power Analysis, SPA, or Differential Power Analysis, DPA) or measuring the execution time. In addition, attacks are possible that exploit unintended behaviour of the TOE in case of fault induction (Differential FaultAnalysis, DFA).
  - The TSF F.RNG (Physical random number generator, online test, acc. AIS31).
  - The TSF F.RNG_Access (Pseudo-random number generator, acc AIS20).

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for: F.RSA, F.RSA_KeyGen, F.HW_DES, F.DES and F.SHA-1.

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2). But Cryptographic functions with a security level of 80 bits or lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore for these functions it shall be checked whether the related crypto operations are appropriate for the intended system.

Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (www.bsi.bund.de).

The cryptographic functions 2-key Triple DES (2TDES), RSA 1024, SHA1 used as collision-resistent hash function, provided by the TOE have got a security level of maximum 80 Bits (in general context).

A recommended usage of RSA according to [28] uses at least 1536 Bits until the end of 2009. The TOE offers up to 2048 Bits for RSA.

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2, especially the User Guidance [15] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Security Target

For the purpose of publishing, the Security Target Lite [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Errichtungsgesetz
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
DES	Data Encryption Standard; symmetric block cipher algorithm
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
GDS	Graphic Design System; Image file format used for integrated circuit masks
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, Adelmann – a public key encryption algorithm
RSA-CRT	RSA algorithm using the Chinese Remainder Theorem

SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SOF	Strength of Function
SSMC	Systems on Silicon Manufacturing Co. Pte. Ltd., Singapore
ST	Security Target
TOE	Target of Evaluation
Triple-DES	Symmetric block cipher algorithm based on the DES
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TSS	TOE Summary Specification

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.[8]

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target BSI-DSZ-CC-0584-2009, Version 1.2, 08 January 2009, P5CC036V1D, NXP Semiconductors Germany GmbH (confidential document)

[7] Evaluation Technical Report, V1.5, 20 March 2009, NXP P5CC036V1D Secure Smart Card Controller with Cryptographic Library, T-Systems GEI GmbH (confidential document)

[8] Configuration list for the TOE, Version 2.0, 31 January 2009, Crypto Library on the P5CC036V1D (confidential document)

[9] Security Target Lite BSI-DSZ-CC-0584-2009, Version 2.2, 08 January 2009, Secured Crypto Library on the P5CC036V1D, NXP Semiconductors Germany GmbH (sanitised public document)

[10] Protection Profile BSI-PP-0002-2001, Version 1.0, July 2001, by Atmel Smart Card ICs, Hitachi Europe Ltd., Infineon Technologies AG, Philips Semiconductors

[11] ETR-lite for composition according to AIS 36 for the Product Secured Crypto Library on the P5CC036V1D, 1.4, 23 January 2009, T-Systems GEI GmbH (confidential document)

[8] Specifically

- AIS 20, Version 1, 2 December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 3, 6 August 2007, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 3, 6 August 2007, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[12] Philips Semiconductors Data Sheet: SmartMX – P5CC036 Secure Smart Card Controller, Revision 3.3, 27 June 2005, NXP Semiconductors Germany GmbH

[13] Philips Semicunductors Documentation: Instruction Set SmartMX-Family, Secure Smart Card Controller, Objective Specification, Revision 1.1, 04 July 2006, NXP Semiconductors Germany GmbH

[14] NXP Semiconductors Guidance, Delivery and Operation Manual for the P5CC009V1D, P5CC036V1D of Secure Smart Card Controller, NXP Semiconductors, Version 1.2, 08 January 2009, NXP Semiconductors Germany GmbH

[15] NXP Semiconductors User Guidance: Secured Crypto Library on the P5CC036V1D, Revision 2.2, 08 January 2009, NXP Semiconductors Germany GmbH

[16] NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Pseudo Random Number Generator & Chi-Squared Test Library, Revision 3.0, 23 November 2005, NXP Semiconductors Germany GmbH

[17] NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Secured DES Library, Revision 2.0, 23 November, 2005, NXP Semiconductors Germany GmbH

[18] NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – SHA-1 Library, Revision 3.0, 23 November 2005, NXP Semiconductors Germany GmbH

[19] NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Secured RSA Library, Revision 3.0, 23 November, 2005, NXP Semiconductors Germany GmbH

[20] NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Secured RSA Key Generation Library, Revision 3.0, 23 November 2005, NXP Semiconductors Germany GmbH

[21] Philips Semiconductors Software Delivery Description: Crypto Library on SmartMX, Secured Random Number Library, CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, 23 November 2005, NXP Semiconductors Germany GmbH

[22] Philips Semiconductors Software Delivery Description: Crypto Library on SmartMX, Secured DES Library, CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, 23 November 2005, NXP Semiconductors Germany GmbH

[23] Philips Semiconductors Software Delivery Description: Crypto Library on SmartMX, SHA-1 Library, CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, 23 November 2005, NXP Semiconductors Germany GmbH

[25] Philips Semiconductors Software Delivery Description: Crypto Library on SmartMX, Secured RSA Library, CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, 23 November 2005, NXP Semiconductors Germany GmbH

[26] Philips Semiconductors Software Delivery Description: Crypto Library on SmartMX, Secured RSA Key Generation Library, CC EAL4+ on P5CC036V1D, Delivery Module Contents, Revision 1.0, 23 November 2005, NXP Semiconductors Germany GmbH

[27] Certification Report BSI-DSC-CC-0583-2009 for NXP Smart Card Controller P5CC036V1D and P5CC009V1D each with specific IC dedicated Software, 29 April 2009, BSI

[28] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, Übersicht über geeignete Algorithmen vom 17. Dezember 2007, published at 05 February 2008 in Bundesanzeiger Nr 19, page 376

[29] Security Target BSI-DSZ-0583-2009, Version 1.2, 08 January 2009, P5CC036V1D/ P5CC009V1D, NXP Semiconductors Germany GmbH (confidential document)

[30] Security Target Lite BSI-DSZ-0583-2009, Version 1.2, 08 January 2009, P5CC036V1D/ P5CC009V1D, NXP Semiconductors Germany GmbH (sanitised public document)

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	**Assurance Family**
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

D Annexes

List of annexes of this certification report

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0584-2009

Evaluation results regarding development and production environment

The IT product NXP P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software (Target of Evaluation, TOE) has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

As a result of the TOE certification, dated 3 June 2009, the following results regarding the development and production environment apply. The Common Criteria Security Assurance Requirements

- ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.2),
- ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and
- ALC – Life cycle support (i.e. ALC_DVS.2, ALC_LCD.1, ALC_TAT.1),

are fulfilled for the development and production sites of the TOE listed below:

(a) NXP Semiconductors GmbH, Business Line Identification, Georg-Heyken-Str. 1, 21147 Hamburg (Development Center)

(b) NXP Semiconductors (Thailand), Assembly Plant Bankok, Thailand (APB), 303 Moo 3 Chaengwattana Rd. Laksi, Bankok 10210 Thailand (Assembly, Test Delivery)

(c) NXP Semiconductors GmbH, Business Line Identification, Document Control Office, Mikron-Weg 1, A-8101 Gratkorn (Documentation)

(d) Systems on Silicon Manufacturing Co. Pte. Ltd. (SSMC), 70 Pasir Ris Drive 1, Singapore 519527, Singapore (Semiconductor Factory)

(e) Photronics Singapore Pte. Ltd., 6 Loyang Way 2, Loyang Industrial Park, Singapore 507099 (Mask Shop)

(f) Photronics Semiconductors Mask Corp. (PSMC), 1F, No.2, Li-Hsin Rd, Science-Based Industrial Park, Hsin-Chu City Taiwan R.O.C. (Mask Shop)

(g) NXP Semiconductors GmbH, IC Manufacturing Operations – Test Center Hamburg (IMO TeCH), Stresemannallee 101, 22529 Hamburg (Assembly, Test, Delivery)

(h) NedCard B.V., Bijsterhuizen 25-29, 6604 LM Wijchen, The Netherlands (Module Mounting)

The hardware part of the TOE is identified by P5CC036V1D and its specific GDS-file. The nameplate (on-chip identifier) T503D, which can be checked by the customer, is specific for the SSMC (Singapore) production site.For the hardware part of the composite evaluation refer to the list of sites in the report BSI-DSZ-CC-0583-2009 [27].

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]). The evaluators verified, that the Threats, Security Objectives and Requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.